2. The method of claim 1, further comprising the step of receiving a [registration]voter acknowledgment message from a [registrant] voter acknowledging that the [registrant]voter has received the [initialization]registration response message.

3. The method of claim 1, wherein the [initialization]registration request message includes a nonce, a session key and a blinding factor applied to the nonce, and further comprising the step of storing the [initialization]registration request message and the [initialization]registration response message in a recovery database.

4. A method for recovering from an interruption in initializing an electronic voting transaction, comprising the steps of:

a. receiving a first [initialization]registration request message from a [registrant]voter that includes a nonce, a session key, and a blinding factor applied to the nonce, and that atomically binds

i. vote authorization data, and

ii. a blinded unvalidated vote certificate to be validated;

b. storing the [initialization] registration request message in a recovery database;

c. determining if the vote authorization data is valid;

d. if the vote authorization data is valid, then validating the blinded unvalidated vote certificate to obtain a blinded validated vote certificate;

e. sending a first [initialization]registration response message to a [registrant]voter that includes the blinded validated vote certificate atomically bound to the [initialization]registration request message[received in step a];

f. storing the first [initialization]registration response message in a recovery database;

g. receiving a second [initialization]registration request message;

h. determining if the second [initialization]registration request message has the same nonce, session key, and blinding factor applied to the nonce as the first [initialization]registration request message stored in the recovery database; and

i. if the second [initialization]registration request message has the same nonce,

session key, and blinding factor applied to the nonce as the first [initialization]registration request message, then

1. retrieving the first [initialization]registration response message from the recovery database; and
2. sending the first [initialization]registration response message to the [registrant]voter.

5. A method for performing an electronic voting transaction, comprising the steps of:
   a. receiving a voting transaction request message that atomically binds
      i. an unblinded vote certificate, and
      ii. a blinded unvalidated vote certificate to be validated;
   b. determining if the unblinded vote certificate is valid; and
   c. if the unblinded vote certificate is valid, then performing a vote transaction response that includes:
      i. validating the blinded unvalidated vote certificate to obtain a validated blinded vote certificate, and
      ii. sending the validated blinded vote certificate atomically bound to the voting transaction request message to a voting transaction response recipient in a vote transaction response message.

6. The method of claim 5, wherein the [transaction response further includes making available a product to a party]vote certificate indicates a yes or a no vote.

7. The method of claim 5, wherein the [transaction response further includes obtaining payment for a product] parity of the certificate indicates a yes or a no vote.

8. The method of claim 5, further comprising the step of receiving a transaction acknowledgment message from a [registrant acknowledging that the] transaction response recipient acknowledging that the transaction response recipient has received the voting transaction response message.

9. The method of claim 5, further comprising the step of storing the voting transaction request message and the voting transaction response message in a recovery database.

10. A method for recovering from an interruption in an electronic voting transaction, comprising the steps of:

a. receiving a first voting transaction request message that includes a session key, a nonce and a blinding factor applied to the nonce, and that atomically binds
   i. an unblinded vote certificate, and
   ii. a blinded unvalidated vote certificate to be validated;

b. storing the first voting transaction request message in a recovery database;

c. determining if the unblinded vote certificate is valid; and

d. if the unblinded vote certificate is valid, then performing a voting transaction response that includes
   i. validating the blinded unvalidated vote certificate to obtain a validated blinded vote certificate,
   ii. sending the validated blinded vote certificate atomically bound to the voting transaction request message to a voting transaction response recipient in a first voting transaction response message, and
   iii. storing the first voting transaction response message in a recovery database;

e. receiving a second voting transaction request message that includes a session key, a nonce and a blinding factor applied to the nonce, and that atomically binds
   i. an unblinded voting certificate, and
   ii. a blinded unvalidated voting certificate to be validated;

f. determining if the second voting transaction request message has the same nonce, session key, and blinding factor applied to the nonce as the first voting transaction request message stored in the recovery database; and

g. if the second voting transaction request message has the same nonce, session key, and blinding factor applied to the nonce as the first voting transaction request message, then

i. retrieving the first voting transaction response message from the recovery database, and

ii. sending the first voting transaction response message to the voting transaction response recipient.

11. A method for auditing an electronic voting transaction, comprising the steps of:

a. receiving a voting transaction request message that atomically binds

i. an unblinded vote certificate,

ii. a blinded unvalidated vote certificate to be validated, and

iii. blinded vote audit data;

b. sending an vote audit request message atomically bound to the vote transaction request message to [an audit recipient]a voter;

c. receiving an vote audit response message atomically bound to the vote audit transaction message, wherein the vote audit response message includes vote audit response data;

d. determining if the blinded vote audit data is valid using the vote audit response data.

12. The method of claim 11, wherein the vote audit response data is determined to be valid if

i. the vote audit response data corresponds to the blinded vote audit data received in the voting transaction request message, and

ii. the vote audit response data is legitimate.

13. An apparatus for initializing a series of electronic voting transactions, comprising:

a. a processor; and

b. a memory [that stores]storing instructions adapted to be executed by said processor to,

i. receive an [initialization] voter registration request message that atomically binds vote authorization data and a blinded unvalidated vote certificate to be validated;

ii. determine if the vote authorization data is valid;

iii. if the vote authorization data is valid, then to validate the blinded unvalidated vote certificate to obtain a blinded validated vote certificate; and

iv. send [an initialization] a voter registration response message to a [registrant] voter that includes the blinded validated vote certificate atomically bound to the [initialization]voter registration request message,

said memory coupled to said processor.

14. The apparatus of claim 13, [further comprising a port adapted to be coupled to a network, said port coupled to said memory and said processor]wherein the certificate indicates a yes or no vote.

15. An apparatus for performing an electronic voting transaction, comprising:

a. a processor; and

b. a memory [that stores]storing instructions adapted to be executed by a processor to

i. receive a voting transaction request message that atomically binds an unblinded vote certificate and a blinded unvalidated vote certificate to be validated;

ii. determine if the unblinded vote certificate is valid; and

iii. if the unblinded vote certificate is valid, then to perform a vote transaction response that validates the blinded unvalidated vote certificate to obtain a validated blinded vote certificate, and sends the validated blinded vote certificate atomically bound to the voting transaction request message to a [transaction response recipient] voter

in a voting transaction response message,

said memory coupled to said processor.

16. The apparatus of claim 15, [further comprising a port adapted to be coupled to a network, said port coupled to said memory and said processor] wherein the parity of the certificate indicates a yes or a no vote.

17. An apparatus for auditing an electronic voting transaction, comprising:

a. a processor; and

b. a memory [that stores]storing instructions adapted to be executed by said processor to

i. receive a transaction request message that atomically binds an unblinded vote certificate and a blinded unvalidated vote certificate to be validated and blinded vote audit data;

ii. send an vote audit request message atomically bound to the voting transaction request message to [an audit recipient]voter;

iii. receive a[n] vote audit response message atomically bound to the vote audit transaction message, where the vote audit response message includes vote audit response data; and

iv. determine if the blinded vote audit data is valid using the vote audit response data,

said memory coupled to said processor.

18. The apparatus of claim 17, [further comprising a port adapted to be coupled to a network, said port coupled to said processor and said memory]wherein the certificate indicates a yes or no vote.

19. An apparatus for recovering from an interruption in an electronic voting transaction, comprising:

a. a processor; and

b. a memory [that stores]storing instructions adapted to be executed by said processor to

i. receive a first voting transaction request message that includes a session key, a nonce and a blinding factor applied to the nonce, and that atomically binds an unblinded vote certificate and a blinded unvalidated vote certificate to be validated;

ii. store the first voting transaction request message in a recovery database;

iii. determine if the unblinded vote certificate is valid;

iv. if the unblinded vote certificate is valid, then performing a voting transaction response that validates the blinded unvalidated vote certificate to obtain a validated blinded vote certificate, sends the validated blinded vote certificate atomically bound to the voting transaction request message to a voting transaction response recipient in a first voting transaction response message, and stores the first voting transaction response message in a recovery database;

v. receive a second voting transaction request message that includes a session key, a nonce and a blinding factor applied to the nonce, and that atomically binds an unblinded vote certificate and a blinded unvalidated vote certificate to be validated;

vi. determine if the second voting transaction request message has the same nonce, session key, and blinding factor applied to the nonce as the first voting transaction request message stored in the recovery database;

vii. if the second voting transaction request message has the same nonce, session key, and blinding factor applied to the nonce as the first voting transaction request message, then to retrieve the first voting transaction response message from the recovery database and send the first voting transaction response message to the voting transaction response recipient,

said memory coupled to said processor.

20. The apparatus of claim 19, [further comprising a port adapted to be coupled to a network, said port coupled to said processor and said memory]wherein the parity of the certificate indicates a yes or a no vote..

21. A medium [that stores]storing instructions adapted to be executed by a processor to perform the steps of:

a. receiving a[n initialization] voter registration request message that atomically binds

i. vote authorization data, and

ii. a blinded unvalidated vote certificate to be validated;

b. determining if the vote authorization data is valid;

c. if the vote authorization data is valid, then validating the blinded unvalidated vote certificate to obtain a blinded validated vote certificate; and

d. sending a[n initialization] voter registration response message to a [registrant] voter that includes the blinded validated vote certificate atomically bound to the [initialization]voter registration request message[received in step a].

22. A medium [that stores]storing instructions adapted to be executed by a processor to perform the steps of:

a. receiving a voting transaction request message that atomically binds

i. an unblinded vote certificate, and

ii. a blinded unvalidated vote certificate to be validated;

b. determining if the unblinded vote certificate is valid; and

c. if the unblinded vote certificate is valid, then performing a voting transaction response that includes

i. validating the blinded unvalidated vote certificate to obtain a validated blinded vote certificate, and

ii. sending the validated blinded vote certificate atomically bound to the

voting transaction request message to a voting transaction response recipient in a voting transaction response message.

23. A medium [that stores]storing instructions adapted to be executed by a processor to perform the steps of:

a. receiving a voting transaction request message that atomically binds

i. an unblinded vote certificate,

ii. a blinded unvalidated vote certificate to be validated, and

iii. blinded vote audit data;

b. sending a[n] vote audit request message atomically bound to the voting transaction request message to a[n audit recipient]voter;

c. receiving a[n] vote audit response message atomically bound to the vote audit transaction message, wherein the vote audit response message includes vote audit response data;

d. determining if the blinded vote audit data is valid using the vote audit response data.

24. A system for performing an electronic voting transaction, comprising:

a. means for receiving a voting transaction request message that atomically binds

i. an unblinded vote certificate, and

ii. a blinded unvalidated vote certificate to be validated;

b. means for determining if the unblinded vote certificate is valid; and

c. means for validating the blinded unvalidated vote certificate to obtain a validated blinded vote certificate; and

d. means for sending the validated blinded vote certificate atomically bound to the voting transaction request message to a [transaction response recipient]voter in a voting transaction response message.

25. The system of claim 24, further comprising means for auditing an electronic voting transaction.